UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

JOSEPH ZAGACKI, individually and on behalf of all others similarly situated, Plaintiff, v. COMCAST CABLE COMMUNICATIONS, LLC d/b/a XFINITY CITRIX SYSTEMS, INC., and, CITRIX SYSTEMS, INC. Defendant.	Case No. **CLASS ACTION COMPLAINT**

Plaintiff Joseph Zagacki ("Plaintiff"), by the undersigned counsel, files this Class Action Complaint, individually and on behalf of a class of all similarly situated persons, against Defendants and Comcast Cable Communications, LLC d/b/a Xfinity ("Comcast") and Citrix Systems, Inc. ("Citrix") (collectively "Defendants"). The following allegations are based upon Plaintiff's personal knowledge with respect to himself and his own acts, and on information and belief as to all other matters.

INTRODUCTION

1. Plaintiff and Class Members bring this class action against Defendants for their failures to adequately secure and protect the personally identifiable information ("PII") of Plaintiff and Class Members, including but not limited to names, mailing addresses, telephone numbers, dates of birth, partial Social Security numbers, usernames and encrypted passwords, as well as security question prompts and responses.

2. Comcast is a telecommunications business that markets a range of consumer products including cable television, internet, telephone, and wireless services.

3. Citrix provides cloud computing services to over 16 million cloud users, and thousands of organizations. Its services include but are not limited to server technologies, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing technologies.

4. Comcast, as a substantial telecommunications and cable provider, and Citrix, as a substantial technology services company, both have the resources to take seriously the obligation to protect their customers' PII. However, Defendants failed to invest the time or resources necessary to protect the PII of Plaintiff and Class members.

5. This class action is brought on behalf of all citizens of all states in the United States who are the victims of a targeted cyberattack on Defendants that occurred between October 16th and 19th , 2023 ("the Data Breach").

6. On October 10, 2023, Citrix announced the vulnerability in the software product used by Comcast and thousands of other companies, known as the "Citrix Bleed" vulnerability, which has been exploited by ransomware cybercriminals.[1]

7. Comcast began publicly disclosing a Notice of Data Security Incident to Plaintiff and the Class Members a full two months after the breach, on December 18, 2023.[2] As a result of Defendants' inability to properly secure Plaintiff and the Class Members' PII, data thieves were able to access and obtain the PII of Plaintiff and Class Members.

[1] What Is Citrix Bleed? The Next Ransomware Patch You Need, Government Technology (Dec. 6, 2023), https :/ /www .govtech.com/security/what-is-citrix-bleed-the-next-ransomware-patch-you-need (last visited January 30, 2024).

[2] *Notice to Customers of Data Security Incident,* available at https://assets.xfinity.com/assets/dotcom/learn/ Data Incident.pdf (last visited January 30, 2024).

8. The December 18th Notice failed to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed the Class Members' PII, what Citrix product contained the vulnerability, and whether the breach was a system-wide breach or limited to a certain subset of customers.

9. The Notice also failed to provide details on how many people were impacted by the Data Breach. In a filing with the Maine Attorney General's Office, Comcast stated that the Data Breach affected 35.8 million people.

10. Defendants knowingly collected the PII of customers in confidence, and have a resulting duty to secure, maintain, protect, and safeguard that PII against unauthorized access and disclosure through reasonable and adequate security measures.

11. Plaintiff and Class Members entrusted their PII to Defendants, their officials, and agents. That PII was subsequently compromised, unlawfully accessed, and stolen due to the Data Breach.

12. Defendants breached their duties by negligently and recklessly maintaining the PII of Plaintiff and Class Members. It is believed that the means of the data breach and the risk of improper disclosure were known and foreseeable to the Defendants. Their failure to secure the PII left it in a dangerous and vulnerable state.

13. Defendants also neglected proper monitoring of the computer network and systems containing the PII. Adequate monitoring could have detected the intrusion sooner or prevented it altogether. This negligence has heightened the risk of exposure for Plaintiff and Class Members, as their identities are now in the hands of data thieves due to Defendants' actions.

14. Defendants neglected to provide sufficient notice of unauthorized access to the PII by a cyber attacker and failed to specify the information accessed and stolen.

15. Data thieves can potentially use the accessed PII to commit various crimes, including fraud, opening financial accounts, obtaining loans, filing fraudulent tax returns, and providing false information during arrests.

16. As a result of the Data Breach, Plaintiff and Class Members have suffered and continue to face a heightened and imminent risk of fraud and identity theft, requiring constant monitoring of their financial accounts.

17. As a result of the Data Breach, Plaintiff and Class Members have suffered ascertainable losses, including, but not limited to, a loss of potential value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendants, out-of- pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

18. The invasion of property interest in their PII entitles Plaintiff and Class Members to damages from Defendants. These harms are ongoing, and future damages are expected as thieves continue to misuse the information for several years. To protect themselves, Plaintiff and Class Members may incur out-of-pocket costs for credit monitoring services, credit freezes, credit reports, and other protective measures.

19. Plaintiff files this lawsuit seeking redress for these issues on behalf of Plaintiff and all putative Class Members who were affected by the Data Breach.

PARTIES

20. Plaintiff Joseph Zagacki ("plaintiff") is a resident of Philadelphia, PA, and a citizen of Pennsylvania. Mr. Zagacki has been a customer of Xfinity since 2011.

21. Defendant Comcast Cable Communications, LLC d/b/a Xfinity is a Delaware limited liability company with its principal place of business located in Philadelphia, Pennsylvania.

22. Defendant Citrix Systems, Inc. is a Delaware corporation with its principal place of business located in Fort Lauderdale, Florida.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C.§ 1332(d)(2)(A). The amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendants.

24. This Court has personal jurisdiction over Defendant Comcast because Comcast is a citizen and resident of this Commonwealth and whose principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

25. This Court has personal jurisdiction over Defendant Citrix Systems, Inc. because Plaintiff's claims arise out of Defendant's contacts with this Commonwealth, and Defendant's contacts with this Commonwealth are substantial.

26. Venue is proper under 18 U.S.C § 139l(b)(l) because Comcast resides in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, and Defendants conduct substantial business in this District.

FACTUAL BACKGROUND

A. Defendant Citrix's Business

27. Established in 1989, Citrix is a global cloud computing company offering technology services to numerous organizations. Its diverse range of services includes server technologies, application and desktop virtualization, networking, software as a service (SaaS), and

cloud computing technologies. Citrix boasts a substantial client base, with claims of serving over 16 million cloud users.

28. With a widespread client portfolio, Citrix caters to thousands of companies globally.[3] In the United States, it services extend across various sectors such as education, energy and utility, financial services, government and public sector, healthcare, insurance, manufacturing, childcare, professional services, retail, technology, telecommunications, and transportation.[4] Through contracts with these clients, Citrix accumulates and stores the PII of millions of individuals in its databases.

29. According to the company, Citrix's digital workspace solutions are relied upon by more than 400,000 companies worldwide, including 99 percent of the Fortune 500.[5]

B. Defendant Comcast's Business

30. Comcast is one of the companies that uses Citrix's products.

31. Comcast is an American telecommunications business, which provides a spectrum of consumer products and services, including cable television, internet services, telephone, and wireless services.

32. Comcast divides its business into two segments: Connectivity & Platforms and Content & Experiences.[6] The Connectivity & Platforms segment contains Comcast's broadband and wireless connectivity businesses under the Xfinity and Comcast brands in the United States

[3] Citrix Customer stories, available at https://www.citrix.com/customers/ (last visited January 30, 2024).

[4] *Id.*

[5] Citrix Named to Cloud 500 (Mar. 1, 2022), available at https://www.citrix.com/news/announcements/mar-2022/citrix-named-to-cloud-500.html (last visited February 1, 2024).

[6] Comcast Corporation (Form 10-Q) (Oct. 26, 2023).

and under the Sky brand in certain territories in Europe.[7] The Connectivity & Platforms segment is comprised of both residential and business customers who subscribe to a range of broadband, wireless connectivity and residential and business video services.[8] Comcast generates revenue from the customers who subscribe to these services and the sale of related devices.[9]

33. Comcast earnings report, broke down its customers: 32.3 million Broadband customers, 14.9 million video customers, and 5.9 million wireless customers.[10]

34. The Comcast makes several representations to its customers regarding the strength of its cybersecurity infrastructure, including that Comcast "help[s] protect you with multiple layers of security that automatically detect and block hundreds of thousands of cyber events every second," and "follow[s] industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain.[11]

35. However, Comcast fell far short of meeting its duty to safeguard the millions of pieces of customer PII.

36. Comcast became aware of a vulnerability in one of the software products used by Xfinity on October 10, 2023 and was advised to patch the software *as soon as possible* to prevent serious cybersecurity breaches.[12] However, Comcast failed to take sufficient preventative and protective measures in time, and between October 16 and 19, 2023, unauthorized persons accessed

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] Comcast Reports 2nd Quarter 2023 Results, Comcast Corporation (July 27, 2023).

[11] https://www.xfinity.com/privacy/

[12] https://www.theverge.com/2023/12/18/24007082/xfinity-data-breach-hack-notice-citrix

millions of customer PII stored on Xfinity systems.[13] Comcast belatedly performed the recommended patches on October 23, a few short days after the Breach occurred.

37. Even after performing the software patch, it was only "during a routine cybersecurity exercise on October 25" that Comcast discoverd the cyberattack.[14]

38. Upon information and belief, *nearly all* Xfinity customers in the U.S. had their PII accessed during this Breach.[15]

39. Only in mid-December, more than *two months* after the Breach occurred, did Comcast belatedly publish a general Notice regarding the incident (the "Notice"), despite conducting an investigation and concluding as early as November 16, 2023 that customer PII had been accessed.

40. According to the Notice, Comcast "notified federal law enforcement and conducted an investigation into the nature and scope of the incident" but to date it is wholly unclear what such investigative efforts involved. Upon information and belief, the investigation is still ongoing.

41. The Notice indicated that the hackers accessed and acquired account usernames, hashed passwords, and customer names, contact information, last four digits of social security numbers, dates of birth and secret questions and answers.

42. The Notice is sparse; it does not provide any substantive details about who accessed the system, the exact date of the Breach, the software involved, or Xfinity's efforts to prevent the

[13] https://www.businesswire.com/news/home/20231218979935/en/Notice-To-Customers-of-Data-Security-Incident

[14] *Id.*

[15] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c9a529ab3ca2c.shtml; see also https://www.usatoday.com/story/tech/2023/12/20/xfinity-data-breach-comcast-hack/71982101007/

Breach. Thus, Plaintiff and Class Members are at a disadvantage in trying to determine what actions to take in response to Xfinity's negligent handling of their PII.

43. Due to the ongoing nature of the investigation, it is highly possible that the hackers accessed other pieces of PII, such as bank account and debit or credit information stored on customers' accounts for payment.

44. Not only did the Comcast fail to notify Xfinity customers of the Breach in a timely manner or with any meaningful information, but the "solutions" offered to customers are, at best, inadequate and at worst, moot. First, Comcast required customers to reset their passwords and enable two-factor authentication. However, resetting an account password does nothing to protect the PII that had already been accessed by nonauthorized persons. The Plaintiff's, or any Class Member's, PII could have already been sold or otherwise used for any number of nefarious purposes.

45. Comcast also advised customers to routinely monitor and review financial and other accounts, as well as credit reports.[16] This is no simple task, as Plaintiff and other Class Members have many accounts, online and otherwise, that could be accessed with the PII that was stolen from Xfinity's systems. Such monitoring requires time and effort that Plaintiffs would otherwise not have expended on these matters. Furthermore, given the scant details Comcast has provided about the Breach as it continues its investigation, the burden of discovering possible fraudulent transactions has been shifted to Xfinity customers.

46. Notably, Comcast has not offered free credit monitoring or identity fraud protection to those impacted by the Breach, which firms typically offer their customers following a serious

[16] https://assets.xfinity.com/assets/dotcom/learn/Data_Incident.pdf

data breach. Thus, Comcast indicates an unwillingness to assist or protect its customers from the potential consequences of its own negligence.

C. Defendants were on Notice That Its Systems were Vulnerable to Cyberattack

47. At all relevant times, Defendants were well aware that the PII they collect from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for inappropriate and deceitful purposes.

48. PII is a valuable commodity to cyber attackers. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[17]

49. Defendants were on notice of the vulnerabilities in its cybersecurity systems. It admits that it received notice approximately two weeks before the Breach that its software was vulnerable to attack.

50. Independent of this explicit knowledge, the frequent occurrence of cyberattacks against corporations that collect and store customer PII continues to increase year-over-year, a fact that should have alerted Defendants to potential vulnerabilities and the need to ensure the robustness of its cybersecurity infrastructure.

51. According to the Identity Theft Resource Center, the number of data compromises reported in the first six months of 2023 was higher than the *total* number of compromises reported every year except one in between 2005 and 2020.[18]

---

[17] *What To Know About Identity Theft*, Fed. Trade Comm'n Consumer Advice (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Feb. 1, 2024).

[18] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://www.idthecenter.org/identity-theft-aftermath-study/ (last visited Feb. 2, 2024).

52. In fact, several major communications corporations have reported massive recent data breaches, including US Cellular in January 2023, AT&T and Verizon in March 2023, and T-Mobile in 2021. These corporations provide the same types of services as Comcast and Xfinity. Thus, Comcast knew or should have known that the PII it collects and stores from its customers is the type that hackers are constantly trying to access and misappropriate.

53. Comcast has demonstrated an acute awareness of both the value of customer PII and the importance of securing this PII throughout its Privacy Policy[19], which states, *inter alia*:

> We know you care about your privacy and the protection of your personal information. We also know it is our responsibility to be clear about how we protect your information. We designed this Privacy Policy to do just that. It explains the types of personal information we collect, and how we collect, use, maintain, protect, and share this information. This Privacy Policy also tells you about the rights and choices you may have when it comes to your personal information.
>
> ***
>
> To provide you with our Services, we collect your personal information. This can include information that does not personally identify you — such as device numbers, IP addresses, and account numbers. It may also include information that does personally identify you, such as your name, address, and telephone number. We call any information that identifies you "personally identifiable information" or "PII."
>
> If you allow others to use your Services, we will also collect personal information about those individuals. If you use our Services through someone else's account, we will collect information about you, but it may not identify who you are to us. We may also collect information about you from third parties.We collect this information to provide our Services, communicate with you, respond to your requests, and to tailor our Services to best meet your needs and interests.

[19] The entire Privacy Policy can be found at *Our Privacy Policy*, XFINITY, https://www.xfinity.com/privacy/policy#info-collection (last updated Jan. 1, 2024).

D. Defendant Failed to Implement Reasonable and Appropriate Measures to Prevent the Breach

54. PII of the type involved in the Breach is highly valuable to both its owners and bad actors. Customers use this information to conduct essential daily business such as apply for employment or government benefits, secure financing for major purchases, and engage in other commercial activities with public and private entities. In the wrong hands, it can allow a person to commit harmful and serious crimes such as fraud and identity theft, drain bank accounts, or steal tax refunds. Thus, it is essential that any entity entrusted with such information maintain robust security measures to protect it.

55. Comcast is, and at all relevant times has been, aware that the PII it collects and maintains on behalf of its customers is highly sensitive and requires safeguarding. In fact Comcast explicitly states that it "know[s] [customers] care about [their] privacy and the protection of [their] personal information"[20] and is "committed to protecting [customers'] privacy".[21] And a spokesperson for Xfinity commented that "[w]e take the responsibility to protect our customers very seriously"[22]. This is confirmed in the Xfinity Privacy page where it states "[w]e know you rely on us to stay connected to the people and things you care about most. And your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure…"[23]

56. Comcast's Privacy Policy explicitly states that it employs "technical, administrative, and physical safeguards." [24]

[20] Xfinity Privacy Policy, https://www.xfinity.com/privacy/policy
[21] *Id.*
[22] https://www.theverge.com/2023/12/18/24007082/xfinity-data-breach-hack-notice-citrix
[23] Xfinity Privacy Policy, https://www.xfinity.com/privacy/policy
[24] *Id.*

57. Indeed, as a sophisticated international conglomerate, Comcast was, at all relevant times, aware of the importance of safeguarding its customers' PII from the foreseeable and serious consequences that would occur if its data security systems and computer servers were breached.

58. Despite all, Comcast's safeguards were inadequate and failed on approximately October 16, 2023.

59. Comcast acted negligently in failing to implement adequate safeguards to protect customers' personal information, even after being notified of the risk of a Breach. This failure runs afoul of industry best practices, which include, but are not limited to, regularly testing security systems, ensuring that security updates and patches are routinely implemented.

60. Furthermore, through its failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, Comcast has violated Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. The Federal Trade Commission's ("FTC") document "Protecting Personal Information: A Guide for Business" highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks. These guidelines advise businesses to take the following steps to establish reasonable data security practices: protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large

amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. [25]

E. Plaintiff and Class Members Suffered Damages

61. For the aforementioned reasons, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways.

62. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

63. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

64. In addition to their obligations under state laws and regulations, Defendants owed a common law duty to Plaintiff and Class Members to protect PII entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting

[25] FEDERAL TRADE COMMISSION, Protecting Personal Information: A Guide for Business (October 2016), available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Feb. 2, 2024).

the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

65. Defendants further owed and breached their duties to Plaintiff and Class Members to implement processes and specifications that would detect a breach of their security systems in a timely manner and to timely act upon warnings and alerts, including those generated by their own security systems.

66. As a direct result of Defendants' intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, cyber thieves were able to access, acquire, view, publicize, and/or otherwise cause the misuse and/or identity theft of Plaintiff's and Class Members' PII as detailed above, and Plaintiff and Class Members are now at a heightened risk of identity theft and fraud.

67. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

68. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

69. Plaintiff and Class Members did not receive the full benefit of the bargain for the received telecommunications services. As a result, Plaintiff and Class Members were damaged in

an amount at least equal to the difference in the value of the telecommunications services with data security protection they paid for and the services they received without the data security protection.

70. As a result of the Data Breach, Plaintiff's and Class Members' PII has diminished in value.

71. The PII belonging to Plaintiff and Class Members is private, private in nature, and was left inadequately protected by Defendants who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

72. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite their obligations to protect customer data.

73. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of Plaintiff's and Class Members' PII.

74. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

75. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."

76. Defendants' failures to adequately protect Plaintiff's and Class Members' PII has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Rather than assist those affected by the Data Breach, Defendants are putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

77. As a result of Defendants' failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

78. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

79. Plaintiff brings claims on behalf of himself, and for certain claims, on behalf of the proposed class of:

> All individuals in the United States whose PII was compromised as a result of the data breach reported by Xfinity in December 2023.

80. The following people are excluded from the class: (1) any Judge or Magistrate Judge presiding over this action and the members of their family; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or its parents have a controlling interest and their current employees, officers, and directors; (3) persons who properly execute and file a timely request for exclusion from the class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs counsel and Defendants' counsel, and their experts and consultants; and (6) the legal representatives, successors, and assigns of any such excluded persons.

81. ***Numerosity:*** The proposed class contains members so numerous that separate joinder of each member of the class is impractical. Defendants have identified at least 35.8 million individuals whose PU may have been improperly accessed and compromised in the Data Breach.

82. ***Commonality:*** There are questions of law and fact common to the proposed class. Common questions of law and fact include, without limitation:

a. Whether and when Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining Class Members' PU;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' PU;

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' PU;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiff's and Class Members' damages;

i. Whether Defendants violated the law by failing to promptly notify Class Members that their PII had been compromised;

j. Whether Plaintiff and the other Class Members are entitled to actual damages, extended credit monitoring, and other monetary relief;

k. Whether Defendants violated common law and statutory claims alleged herein.

83. ***Typicality:*** Plaintiffs claims are typical of the claims of the members of the Class. The claims of Plaintiff and Class Members are based on the same legal theories and arise from the same unlawful and willful conduct because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

84. ***Policies Generally Applicable to the Class:*** This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible

standards of conduct toward the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect the Class uniformly and Plaintiffs challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

85. ***Adequacy of Representation:*** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

86. ***Superiority:*** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision making.

87. ***Predominance:*** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants

breached their duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

88. ***Injunctive Relief*** Defendants has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

89. ***Ascertainability:*** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class against both Defendants)

90. Plaintiff incorporates by reference all proceeding paragraphs as though fully set forth

91. Plaintiff and Class Members were required to submit their PII to Defendants in order to receive telecommunications services.

92. Defendants knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiff and Class Members.

93. As described above, Defendants owed duties of care to Plaintiff and Class Members whose PII had been entrusted with Defendants.

94. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII.

95. Defendants acted with wanton disregard for the security of Plaintiffs and Class Members' PII. Defendants knew or reasonably should have known that they had inadequate data security practices to safeguard such information, and Defendants knew or reasonably should have known that data thieves were attempting to access databases containing PII, such as those of Defendants.

96. A "special relationship" exists between Defendants and Plaintiff and Class Members. Defendants entered into a "special relationship" with Plaintiff and Class Members because Defendants collected the PII of Plaintiff and the Class Members- information that Plaintiff and the Class Members were required to provide in order to receive the telecommunications services.

97. But for Defendants' wrongful and negligent breaches of the duties owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

98. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or reasonably should have known they were failing to meet their duties, and that Defendants' breaches of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

99. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial. herein.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class against both Defendants)

100. Plaintiff incorporates by reference all proceeding paragraphs as though fully set forth.

101. Pursuant to the FTCA (15 U.S.C. §45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

102. Defendants breached their duties to Plaintiff and Class Members under the FTCA (15 U.S.C. §45) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

103. Defendants' failures to comply with applicable laws and regulations constitutes negligence *per se.*

104. But for Defendants' wrongful and negligent breaches of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

105. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or reasonably should have known that they were failing to meet their duties, and that Defendants' breaches would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

106. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class against both Defendants)

107. Plaintiff incorporates by reference all proceeding paragraphs as though fully set forth.

108. Plaintiff and Class Members entered into an implied contract with Defendants when they obtained telecommunications services in exchange for which they were required to provide their PII. The PII provided by Plaintiff and Class Members to Defendants was governed by and subject to Defendants' privacy duties and policies.

109. Defendants agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify Plaintiff and Class Members in the event that their PII was breached or otherwise compromised.

110. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Defendants would use part of the monies paid to Defendants under the implied contracts to fund adequate and reasonable data security practices.

111. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of the implied contract or implied terms between Plaintiff and Class Members and Defendants. The safeguarding of the PII of Plaintiff and Class Members and prompt and sufficient notification of a breach involving PII was critical to realize the intent of the parties.

112. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

113. Defendants breached their implied contracts with Plaintiff and Class Members to protect Plaintiff's and Class Members' PII when they: (1) failed to have security protocols and measures in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide sufficient notice that their PII was compromised as a result of the Data Breach.

114. As a direct and proximate result of Defendants' breaches of implied contract, Plaintiff and Class Members have suffered damages.

herein.

FOURTH CAUSE OF ACTION B
REACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and the Class against Defendant Citrix)

115. Plaintiff incorporates by reference all proceeding paragraphs as though fully set forth

116. This Count is pleaded in the alternative to the breach of implied contract claim above.

117. Upon information and belief, Defendant Citrix entered into contracts with its clients, including Plaintiff's telecommunications service provider, Comcast, to provide software services- including data security practices, procedures, and protocols sufficient to safeguard the PII of Plaintiff and Class Members.

118. These contracts were made for the benefit of Plaintiff and Class Members given the transfer of their PII to Citrix for storage, protection, and safeguarding was the objective of the contracting parties. Therefore, Plaintiff and Class Members were direct and express beneficiaries of these contracts.

119. Defendant Citrix knew that a breach of these contracts with its clients would harm Plaintiff and Class Members.

120. Defendant Citrix breached the contracts with its clients when it failed to utilize adequate computer systems or data security practices to safeguard Plaintiff's and Class Members' PII.

121. Plaintiff and Class Members were harmed by Defendant Citrix's breaches in failing to use reasonable security measures to safely store and protect Plaintiff's and Class Members' PU.

122. Plaintiff and Class Members are therefore entitled to damages in an amount to be determined at trial.

herein.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class against both Defendants)

123. Plaintiff incorporates by reference all proceeding paragraphs as though fully set forth

124. This Count is pleaded in the alternative to the breach of implied contract claim above and the breach of third-party beneficiary claim above.

125. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their PII- PII that has inherent value. In exchange, Plaintiff and Class Members should have been entitled to Defendants' adequate storage and safeguarding of their PII.

126. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

127. Defendants profited from Plaintiff's and Class Members' retained PII and used their PII for business purposes.

128. Defendants failed to store and safeguard Plaintiff's and Class Members' PII. Thus, Defendants did not fully compensate Plaintiff and Class Members for the value of their PII.

129. As a result of Defendants' failures, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate services without reasonable data privacy and security practices and procedures that they received.

130. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement--or adequately implement- the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

131. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by Defendants.

132. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiffs attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is hereby demanded for all claims so triable.

Dated: February 2, 2024

GLANCY PRONGAY & MURRAY LLP

By: */s/Lee Albert*
Lee Albert (PA ID # 046852)
230 Park Avenue, Suite 358
New York, NY 10169
Tel: (212) 682-5340
Fax: (212) 884-0988
lalbert@glancylaw.com

Attorneys for Plaintiff and the Proposed Class